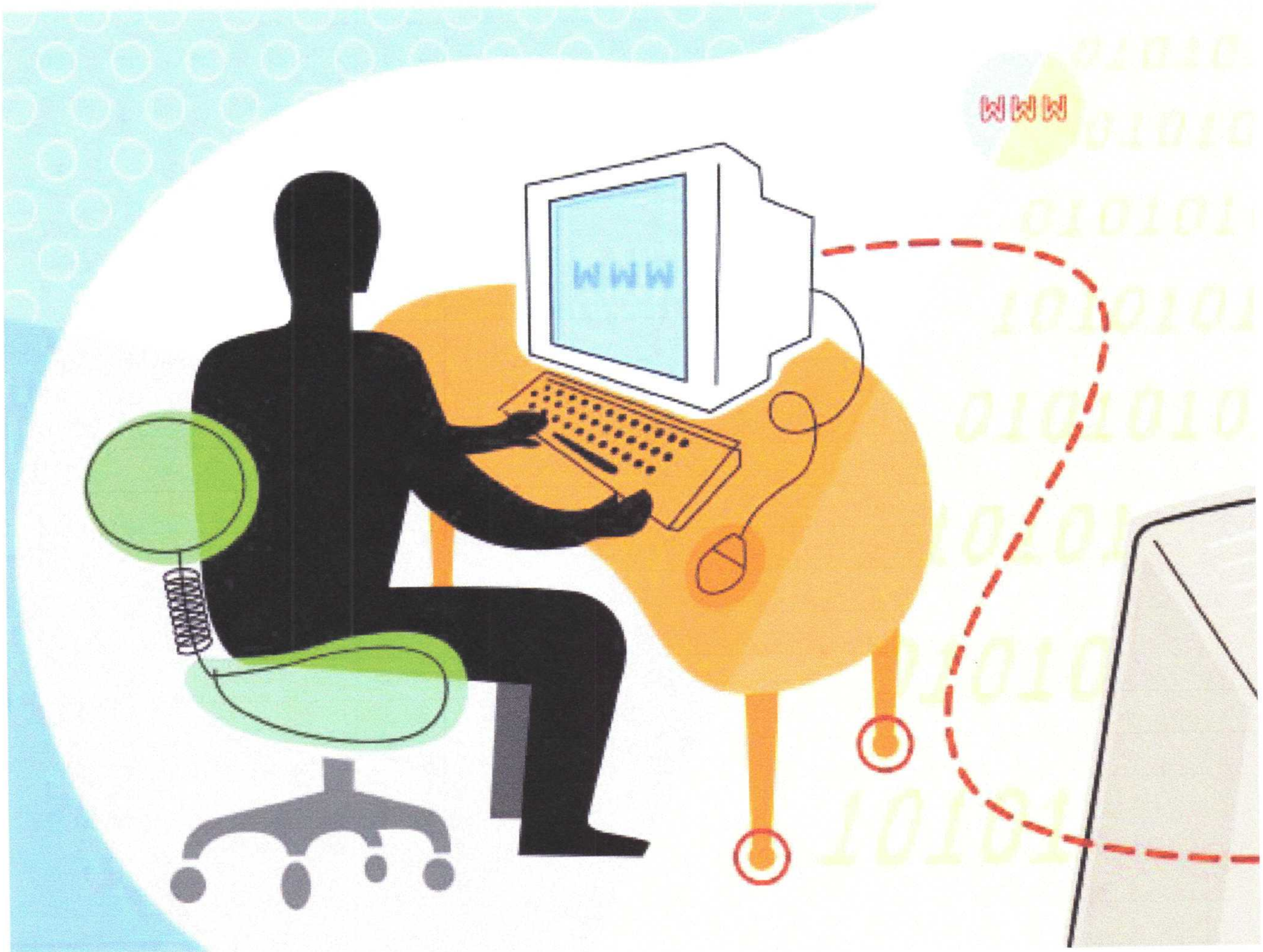


FEDERAL INTERNET

"In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately.

Cellular phones are subject to monitoring, e-mail is easily intercepted and transactions over the Internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number or bank account number puts each of us at risk. Moreover, when we employ electronic methods of communication, we often leave electronic "fingerprints" behind, fingerprints that can be traced back to us.

Whether we are surveilled by the government, criminals or neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb." *Bernstein v. Dept. of Justice*, 176 F.3d 1132, 1145-1146 (9th Cir. 1999).

Invasion of privacy on the Internet encompasses many different areas—the collection and distribution of personal information (including "data mining" and "online profiling"), interception of online transmissions and certain common law invasions like "intrusion into seclusion" and "publication of private facts." There is no comprehensive federal law governing Internet privacy.

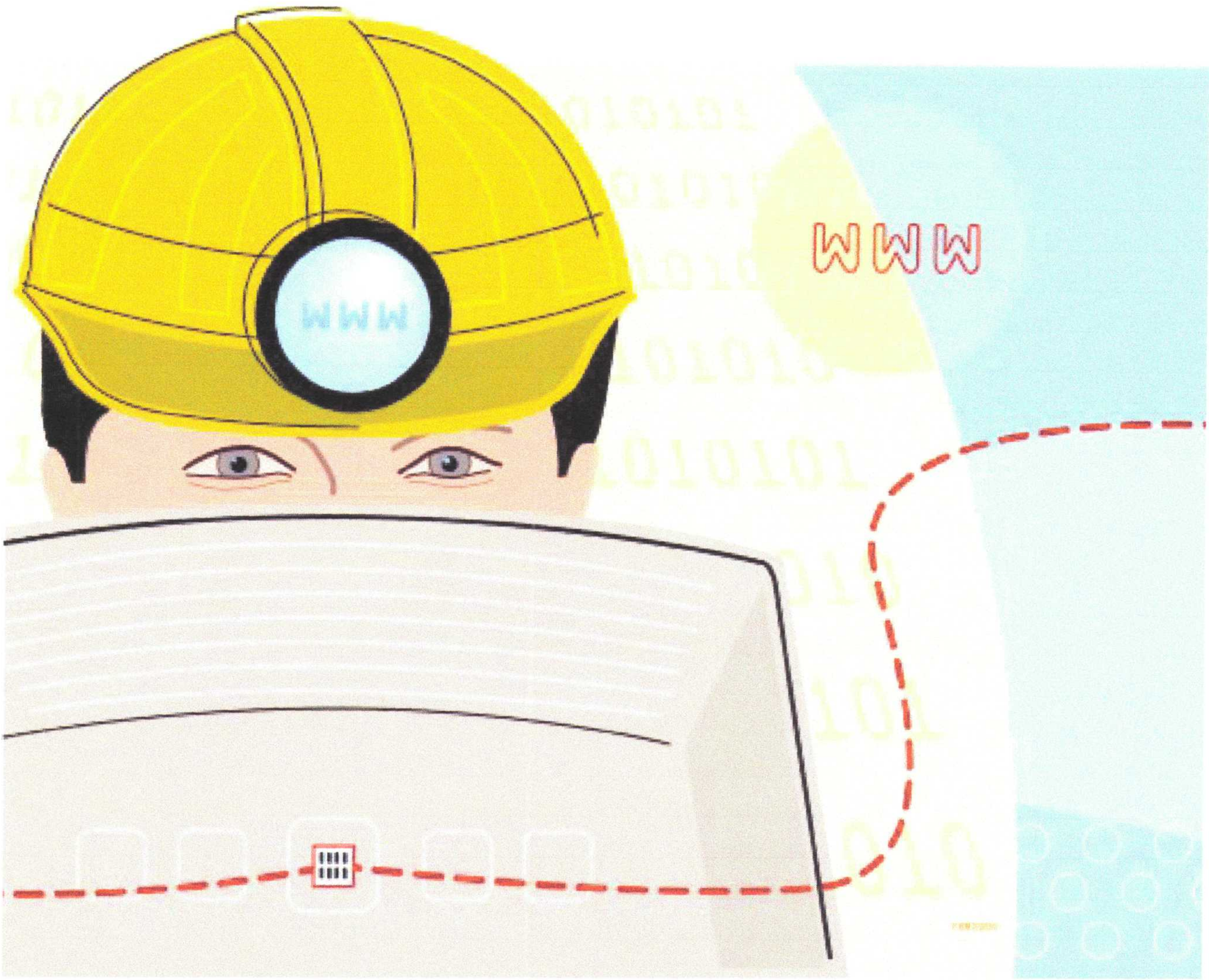


Illustration by Ryon Edwards

PRIVACY LAW

By Edward Fenno

Similarly, there is no comprehensive federal law governing privacy in general. Internet privacy (and privacy in general) in the United States is protected by means of a "sectoral" system, combining legislation, self-regulation, federal and state Constitutional provisions, and common law. Moreover, since many Internet privacy issues are still relatively new, the law in the area is in a state of flux. Nearly every week a new statute, regulation, policy statement or agreement is announced that significantly affects the treatment of Internet privacy.

PERSONAL INFORMATION ON THE INTERNET

"Data mining," "online profiling" and "cookies" have all been major topics of discussion recently, at both a legislative and commercial level. "Data mining" is the collection of personal information on the Internet. "Online profiling" is the practice of recording online behavior for the production of tailored advertising. This profiling is done in part by reading "cookies"—small text files that are generated by the Web server of the site visited, and then stored on the visitor's computer for future reference by the Web site when the visitor visits the site again.

Cookies contain information about what Web pages the Internet user (surfer) viewed, what language he or she speaks and what

selections the surfer made when visiting a particular site. Internet service providers (ISPs) like America Online can also track a surfer's navigation on the Internet using "click-stream" data—electronic records of user activity.

Due to the lack of a comprehensive federal Internet privacy law, corporations, legislators and litigants have been struggling with issues concerning what personal information can be collected about someone online, how the information is collected, whether the person should be notified about the collection and how the person can delete the information collected.

CONSTITUTIONAL PRINCIPLES

There is no explicit general right to privacy set forth in the U.S. Constitution. Several provisions of the Constitution have been held to protect certain "privacy" rights of individuals, however. Still, these provisions do not encompass all types of privacy. Moreover, the protections afforded by the Constitution are only with regard to governmental invasion of privacy (including lawmaking), not invasion by other people.

The Fourth Amendment to the Constitution may provide some protection from collection and distribution of online personal data by the government. For information to be protected by the Fourth Amendment, the individual must have a "legitimate expectation of privacy" that has been invaded by government action. To find this "legitimate expectation," the individual must satisfy a two part test: (1) "the individual, by his conduct, [must have] exhibited an actual (subjective) expectation of privacy ... [i.e.,] the individual has shown that he seeks to preserve something as private"; and (2) "the individual's subjective expectation of privacy [must be] one that society is prepared to recognize as 'reasonable' ... [i.e.,] the individual's expectation, viewed objectively, is 'justifiable' under the circumstances." *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

Certain information on the Internet may pass this test. In 1996, a military court held that an individual does have a legitimate expectation of privacy under the Fourth Amendment in his or her e-mail communications stored and sent via an online service.

The U.S. Supreme Court has held, however, that there is no Fourth Amendment protection of personal information conveyed to third parties for commercial use. *Id.* at 743-744; *U.S. v. Miller*, 425 U.S. 435, 442-444 (1976). People are seen to have "assumed the risk" that the receiver of the information will disclose it to the government. Since Internet users voluntarily make much of their personal information available to third parties in the flow of commerce (e.g., credit card and social security numbers, names, addresses, e-mail addresses), Fourth Amendment protection from government review and use of such information is likely to be limited.

On the other hand, constitutional provisions such as the Commerce Clause and the First Amendment have already been used to strike down state laws concerning Internet privacy. *See, e.g., ACLU of Georgia v. Miller*, F. Supp. 1228 (N.D. Ga. 1997) (Georgia statute precluding anonymous use of Internet struck down as violative of First Amendment); *State v. Heckel*, Superior Court of the State of Washington, King County, March 10, 2000 (Washington's anti-spam statute struck down pursuant to Commerce Clause).

FEDERAL STATUTES

Even though there is no comprehensive federal Internet privacy law, there are a number of federal statutes that may affect the collection and distribution of personal information on the Internet. Several of these statutes primarily concern the interception of online transmissions and will be discussed later. Of the remaining statutes, the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley [financial institutions privacy] Act, the Privacy Act, the Freedom of Information Act, the Fair Credit Reporting Act and the Privacy Protection Act are the most likely to affect collection and distribution of personal information.

In 1998, Congress passed the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501, *et seq.*, which went into effect in April 2000. The Act requires that all commercial Web sites "directed to" children under the age of 13, or that have "actual knowledge" that they collect "personal information" from children (including names, addresses, hobbies, telephone numbers, e-mail addresses and other items), comply with numerous notice, parental consent and disclosure requirements. "Collection" includes not only the requesting of personal information, but also the passive reception of personal information using a message board, chat room or passive tracking device (like a cookie).

If COPPA is found to apply to a Web site or online service, the operator must: (1) provide notice on the Web site or online service of what information it collects from children, how it uses such information and its disclosure practices for such information; (2) obtain verifiable parental consent prior to any collection, use or disclosure of personal information from children; (3) provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance; (4) not condition a child's participation in a game, the offering of a prize or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and (5) establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children. *See*, 16 C.F.R. § 312.3.

The Gramm-Leach-Bliley Act (GLBA) is a new federal law that contains extensive privacy provisions concerning the collection and distribution of personal and financial information by banks, insurers, securities firms and other "financial institutions." (The privacy provisions of the Act can be found at 15 U.S.C. § 6801, *et. seq.*, with corresponding regulations at 12 C.F.R. § 40.) Under the Act, subject to certain exceptions, financial institutions must: (1) establish appropriate safeguards for the protection and confidentiality of customer records; (2) provide an "opt

out" notice to "consumers" (under the Act, "consumers" include people who have applied for a loan or used the financial institution's automatic teller machines but who have not become "customers" of the financial institution by opening an account, having the loan approved, etc.) before sharing their personally identifiable financial information with nonaffiliated third parties; (3) adopt a privacy policy for consumers, and provide it to all customers of the financial institution upon establishing a customer relationship; and (4) include in the privacy policy: (a) the categories of people to whom the non-public personal information collected by the institution can be disclosed, (b) the policies and practices of the institution with respect to disclosing nonpublic personal information of people who have ceased to be customers, (c) the categories of nonpublic personal information collected, and (d) the institution's confidentiality and information security policies, among other things. *See*, 15 U.S.C. §§ 6801-6809; 12 C.F.R. § 40.

Pursuant to the provisions of the GLBA, customers of financial institutions would thus be able to prevent the institutions from providing their personal financial information to e-mail marketers or online profilers. Importantly, financial institutions need not comply with these privacy provisions until July 1, 2001, even though the effective date of the provisions is November 13, 2000.

The Privacy Act, 5 U.S.C § 552a, protects United States citizens and aliens lawfully admitted for permanent residence against unauthorized disclosure of information about them that is held by government agencies. The Act prohibits the disclosure by government agencies of any "records" concerning personal information about an individual to any person or government agency without the prior written consent of the individual. The prohibition is subject to several important exceptions, including: (1) use compatible with the purposes for which the information was collected, (2) civil or criminal law enforcement activity and (3) the health or safety of an individual.

"Records" are defined as "any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history and criminal or employment history and that contains his name, or the identifying number, symbol or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

The Act additionally requires that agencies provide individuals with access to their records, as well as the opportunity to challenge their contents. Moreover, agencies must "establish appropriate administrative, technical and physical safeguards to insure security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity. . . ." *See*, 5 U.S.C. §§ 552a(d), 552a(e).

The Freedom of Information Act (FOIA), 5 U.S.C. § 552, permits broad public access to government records. "Records" are defined in the Act to include information in "electronic format." "To the extent required to prevent a clearly unwarranted invasion of personal privacy," however, the government may "delete identifying details" when it makes available many of its records. 5 U.S.C. § 552(a)(2)(E). This deletion must be justified in writing. Furthermore, FOIA does not permit access to records concerning "trade secrets and commercial or financial information obtained from a person and privileged or confidential." *Id.* at § 552(b)(4). Nor does the Act authorize access to "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." *Id.* at § 552(b)(6).

The Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681, *et seq.*, regulates the use of data associated with personal credit and credit reports. The Act essentially prohibits consumer reporting agencies from disclosing "consumer reports" unless the recipient either has a legitimate business purpose for the information or the reporting agency has received the consent of the individual who is the subject of the reports. 15 U.S.C. §§ 1681a, 1681b. Legitimate business purposes for disclosure include court orders, evaluations for credit, insurance reasons and employment matters.

The FCRA also imposes requirements on users of consumer reports. Users of consumer reports must advise the subjects of the reports when they take adverse actions based on the report. *Id.* at § 1681m. Upon written request from the consumer, users of consumer reports must disclose any basis for adverse action other than the credit report. *Id.* at § 1681n.

The Privacy Protection Act (PPA), 42 U.S.C. §§ 2000aa, *et seq.*, makes government seizure of "work product materials" from "a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast or other similar form of public communication in or affecting interstate or foreign commerce" a criminal offense, unless there is probable cause to believe that the person possessing such materials is committing the offense to which the materials relate. 42 U.S.C. § 2000aa(a). The PPA may prove important in Internet privacy cases in the United

The Fourth Amendment to the Constitution may provide some protection from collection and distribution of online personal data by the government. For information to be protected by the Fourth Amendment, the individual must have a "legitimate expectation of privacy" that has been invaded by government action.

States since it appears facially that nearly everyone posting messages on the Internet or with online services is covered by the Act.

SELF-REGULATION

Rather than enacting a comprehensive federal statue regulating the collection of all personal information from adults, the federal government has encouraged self-regulation. In this regard, the Federal Trade Commission has recently approved a self-regulatory agreement by a consortium of major Internet advertisers to regulate what information they gather from Web surfers and how they use it.

The agreement sets forth three standards for how such companies will gather information anonymously from Web users and use it to profile consumers. Pursuant to the agreement, consumers will be: (1) allowed to opt out of the collection of anonymous data on the Internet for the purpose of profiling; (2) given a chance to determine if they want to allow previously collected anonymous data to be merged with personally identifying information; and (3) allowed to give permission for the collection of personally identifying information at the time and place it is gathered on the Internet.

Many companies not subject to this agreement also maintain "privacy policies" on their Web sites—including notice, choice (opt in/out), access and security provisions—to engender trust with consumers in hopes of making them customers. A study recently quoted in the *Wall Street Journal* reveals that 38 percent of Web users surveyed claim always to read privacy policies and as many as 61 percent of users of financial services sites chose not to use such sites because the users were unsure about how their personal information would be handled by the site.

Further incentive for self-regulation is the European Union's Data Protection Directive. Under this European law, U.S. companies are only entitled to collect, record or disclose online personal data concerning European nationals if the U.S. companies comply with strict privacy "principles" concerning notification, choice, disclosure, security, access and enforcement. *See,* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, Eur. O.J. L281/31 (Nov. 23, 1995), and subsequent "Safe Harbor" principles of July, 2000. The U.S. companies must register their intent to comply with these principles with the U.S. Federal Trade Commission, which then monitors the compliance.

A final incentive for careful self-regulation is the common law. While beyond the scope of this article, it should be noted that Internet privacy is subject to common law invasion of privacy tort actions such as publication of private facts, intrusion into seclusion, misappropriation of name or likeness and false light publicity (although the tort of false light has not been recognized in South Carolina).

Other common law causes of action, such as breach of duty of confidentiality, breach of contract, breach of fiduciary duty, negligence, fraud, trespass, conversion and infliction of emotional distress may also apply.

INTERCEPTION OF ONLINE TRANSMISSIONS

Unlike the privacy concerns in the collection and distribution of online personal data, the privacy concerns in computer hacking and other interceptions of online transmissions have been heavily legislated by the federal government. Two important federal statutes in this area are the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act.

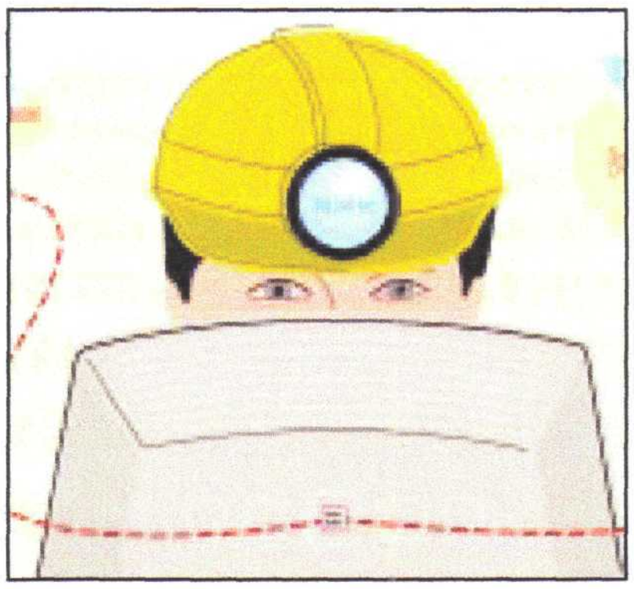
The Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2522, 2701-2709, prohibits the interception of electronic communications, as well as the disclosure or use of intercepted communications. It also protects electronically stored communications from unauthorized access and disclosure, whether by the government or by individuals.

One exception to the statute permits interception of electronic communications made to a system that is "readily accessible to the general public." Thus, the ECPA is not violated when postings to Usenet groups, listservs, bulletin board systems and chat rooms are read and archived. *See,* Susan Gindin, "Lost and Found in Cyberspace," http://www.info-law.com/lost.html, §IV.D.1 (1997).

Another exception allows service providers and anyone else to intercept and disclose an electronic communication where either the sender or the recipient of the message consents to the interception or disclosure. Many commercial services require a consent agreement from new members when signing up for the service, and consent may be implied in employment relationships, especially when the employer notifies employees that their e-mail will be monitored. *Id.*

Finally, the ECPA provides an "ordinary course of business" exception, which may also support employer monitoring of employee e-mail. This exception is found in the definition of "electronic, mechanical or other device," which exempts from the interception prohibition an entity that provides the electronic communication service "in the ordinary course of its business." Cases interpreting the "ordinary course of business" provision have involved telephone monitoring, and the courts have generally held that an employer may monitor an employee for as long as the communication is business-related. *Id.* at n. 259.

Unlike the privacy concerns in the collection and distribution of online personal data, the privacy concerns in computer hacking and other interceptions of online transmissions have been heavily legislated by the federal government.



The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, is primarily intended to prevent unauthorized access to computer networks to protect the privacy of communications associated with those networks. It is also intended to protect the networks from acts of sabotage, such as alteration of data. 18 U.S.C. § 1030. While the CFAA is used primarily against hackers, some litigants have alleged causes of action for violation of the CFAA in spam (unsolicited e-mail) cases as well. Gindin, *supra*, § IV.D.2.

PROTECTING PERSONAL INFORMATION ONLINE

One technique that many Internet surfers use to try to prevent the collection and distribution of their personal information is to use a pseudonym. The right to publish anonymously is protected by the First Amendment. *See, McIntyre v. Ohio Elections Commissions*, 514 U.S. 334 (1995). As noted above, this right has already prevented the enforcement of a state statute that made anonymous Internet communication illegal. Many ISPs will reveal the identity of a subscriber, however, when faced with a subpoena in a lawsuit. Thus, anonymity cannot be relied upon for the protection of an Internet surfer's personal information.

Encryption is another common method by which Internet users protect their privacy. Encryption is the practice of making messages unintelligible to all except the intended recipients. In addition to ensuring secrecy, encryption can be employed to ensure data integrity, authenticate users and facilitate nonrepudiation (e.g., linking a specific message to a specific sender).

Encryption is used on the Internet to protect the privacy of much of the information transmitted online, including credit card numbers. For years, the federal government has restricted the publication of encryption software for fear that foreigners could use the more effective encryption software to conceal from the government communications of terrorists, drug smugglers or others intent on taking hostile action against the United States. The government has recently eased its restrictions, however, as a result of a number of successful lawsuits challenging the restrictions as violative of the First Amendment.

CONCLUSION

While there is no comprehensive federal law governing the collection and distribution of personal information of adults on the Internet, the Children's Online Privacy Protection Act offers broad protection for children under the age of 13. Adults and teenagers must turn to the common law and to marketplace self-regulation for protection in most instances, although financial institutions and the government are subject to federal laws in this area.

With respect to computer hacking and other interceptions of online transmissions, federal protection under the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act are relatively pervasive. Finally, while encryption has proven to be a strong shield against invasion of privacy on the Internet, anonymity has not.

Edward Fenno is a lawyer with Moore & Van Allen in Charleston. He leads the firm's South Carolina media and Internet law practice and is a member of the firm's Intellectual Property and Information Technology practice groups.